ICT Asset Recovery Standard 8.0

Part 2: Criteria

Released 21.06.2021

Territory Release: United Kingdom

Publication Schedule.
Version 8.0 v3.0 21.06.2021

Standard Owner.
ADISA Certification Limited
UK Company Registration Number 07390092
Data Controller Registration ZA239175

www.adisa.global
www.adisarc.com

Foreword

The ADISA Asset Recovery Standard 8.0 is presented as three documents which are:

Part 1: Introduction and Explanatory Notes.
Part 2: Criteria.
Part 3: Supporting Documents.

This document is Part 2 which contains the criteria that are required to be met to become certified against Standard 8.0. To fully understand the criteria and how to apply them it is recommended to read Part 1 prior to reading Part 2 as this document, when read in isolation, will only provide a list of the requirements for a company to hold ADISA Certification.

Part 1 and Part 2 are publicly available via the ADISA website www.adisa.global.
Part 3 is issued to applicants upon start of certification process.

Should you have any questions regarding this Standard or the certification process you should email enquiry@adisa.global.

Yours Sincerely,

Steve Mellings.
Founder.
ADISA.

Contents

ICT Asset Recovery Standard 8.0

Section 1

Business Credentials

Section 1 Business Credentials

Section Introduction

Within the business process of asset recovery, the use of partners, data processors or sub-processors, to perform all or part of the process is commonplace. This section is specifically focussed on how a data controller or data processor might assess the suitability of a data processor or sub-processor who might be used to perform all or part of the data sanitisation process which forms a key part of the asset recovery process.

ADISA has identified several areas within the general governance of a business which are felt to be crucial to assessing suitability. Section 1 presents those areas as criteria and if the applicant is assessed as having met these criteria this provides assurance to the controller about the legitimacy of the processor's business.

Section 1 Core Principles

- Business governance.
    - Financial stability.
    - Insurances held.
    - Confirmation of licences, certifications and permits held.
    - Health and safety.
- Staff screening.
- Business continuity.

Essential

Ref	Criteria
1.1.1	Applicants shall be able to show credit worthiness via the successful completion of a credit check, typically a Dun and Bradstreet risk indicator of a minimum of 3.

Highly Desirable

Ref	Criteria
1.1.2	Applicants should be able to show credit worthiness via the successful completion of a credit check, typically a Dun and Bradstreet risk indicator of 1 to 2.

Guidance Notes

ADISA performs the Dun and Bradstreet check during every audit.

ADISA acknowledges that there can be occasion when a credit score may not be reflective of current financial strength such as after a merger or acquisition. When there is a dispute based on the Dun and Bradstreet scoring, other credit scoring schemes will be considered, and each assessed on their merits.

Applicable UK GDPR Articles

None.

Essential

Ref	Criteria
1.2.1	Applicants shall hold Employers Liability Insurance.
1.2.2	Applicants shall hold Public Liability Insurance.
1.2.3	Applicants shall hold Professional Indemnity Insurance, or an equivalent insurance policy, which protects the business from claims arising due to a failure within the service offered. A copy of this policy will be required to be reviewed by ADISA to ascertain whether it is fit for purpose.

Highly Desirable

Ref	Criteria
1.2.4	Applicants should hold Product Liability Insurance.

Guidance Notes

Copies of the insurance certificates will be required which will show the facility / company being evaluated.

Applicable UK GDPR Articles

None.

Essential

Ref	Criteria
1.3.1	Applicants shall have a Health and Safety Policy and risk assessments of business activities including on-site and off-site work.
1.3.2	Applicants shall have a written Business Continuity Policy (BCP) which is tested regularly[1] and provide evidence of their most recent test. This BCP needs to include provision for systems failure and facility compromise, for example by flooding, and detail how service provision is maintained including where service is carried out by a sub-processor.

Guidance Notes

[1] As a minimum, the BCP shall be tested annually.

Copies of all policy documents will be required to be submitted. Each policy document shall have a specific version reference and renewal date.

Applicable UK GDPR Articles

Article 28 (1) By having a written BCP the applicant will be able to provide sufficient guarantees that the processing activities will be carried out in accordance with the written authorisation of the data controller despite any events which might impact on the processing activity.

Essential

Ref	Criteria
1.4.1	Applicants shall hold ISO 9001 Quality Management Systems. Last audit report shall be disclosed to ADISA with any non-conformities.
1.4.2	All certifications (such as ISO) shall be disclosed, and reports verified by ADISA. Applicants shall maintain valid certifications of referenced Standards throughout the duration of ADISA certification.
1.4.3	All environmental licences, exemptions and / or permits required to operate in each region of operation shall be disclosed and verified by ADISA for inclusion within the website entry on ADISA site.

Highly Desirable

Ref	Criteria
1.4.4	Applicants should hold ISO 14001 Environmental Management Standard.
1.4.5	Applicants should hold OHSAS 18001 or ISO 45001 Occupational Health and Safety Standard.
1.4.6	Applicants should hold ISO 27001 Information Security Management System which includes the ITAD process within scope.
1.4.7	Any ISOs held should be awarded by a recognised auditing body holding accreditation within the regions operated in. For example, UKAS.

Guidance Notes

Copies of all ISO certificates will be required and where the company under evaluation has multiple sites, evidence that the ISO certification has been carried out on the location / process within scope of this certification is required. Reports should be available for inspection upon request.

Applicable UK GDPR Articles

Article 28 (1) ISO 9001 is a Quality Management System and so adherence to this Standard enables the applicant to evidence sufficient guarantees to the data controller that they are taking appropriate technical and organisational measures through the implementation of a QMS system.

Note: ISO 27001 is not deemed essential for this processing activity as the data controller data is never accessed by the applicant and in this regard is never at risk due to vulnerabilities within the applicant's own network. It is viewed as highly desirable as an indication of good practice for the applicant's own data protection activities on data for which it is a data controller.

Essential

Ref	Criteria
1.5.1	Personnel screening policy document shall be issued and shall include a requirement for all staff who have access to the data processing activities to undergo commercial personnel screening to include the following checks: • Criminal background check. • Proof of ID. • Proof of address. • Proof of ability to work.
1.5.2	All driver's contracts of employment shall state that the driver needs to disclose any changes in their licence / permit whilst in the employment of the applicant.
1.5.3	All employee's contracts of employment shall state that the employee needs to disclose any changes in their status (such as criminal convictions or work permit amendments) whilst in the employment of the applicant.
1.5.4	All employee contracts shall include confidentiality clauses.

Highly Desirable

Ref	Criteria
1.5.5	Personnel screening should be done every 3 years.

Guidance Notes

The objective of personnel screening is to provide the employer with information about staff who operate within their business. Where criminal records exist, the employer should assess the suitability of the employee to start employment. This should be done on a case-by-case basis and follow the Rehabilitation of Offenders Act 1974 and other associated Employment Law which the employer is obligated to follow.

The disclosure of changes to driver and employee employment status are included to protect the employer from a non-disclosure which might have an impact of insurance validity and / or which might necessitate a change in working practice.

Applicable UK GDPR Articles

Article 28 (1) The management of insider threats via a staff vetting process enables the applicant to provide sufficient guarantees to the data controller that they are taking appropriate technical and organisational measures.

Essential

Ref	Criteria
1.6.1	Each applicant wishing to hold and maintain certified status shall sign and comply with the ADISA Member's Code of Conduct.

Guidance Notes

The ADISA Members Code of Conduct was originally created in November 2018 and was approved unanimously at the ADISA Members meeting in December 2018 for immediate introduction. Whilst it is NOT a recognised Code of Conduct under Article 40 of the UK GDPR, it is statement where all parties define expectation between them not only for the purposes of achieving and maintaining certification but also for the purposes of promoting good practice within the asset recovery business process.

Applicable UK GDPR Articles

None.

ICT Asset Recovery Standard 8.0

Section 2
UK GDPR and
UK Data Protection Act 2018
Compliance

Section 2 UK GDPR and UK Data Protection Act Compliance

Section Introduction

This section assesses key aspects of compliance with the UK GDPR and UK Data Protection Act 2018 within this business process.

Section 2 Core Principles

- Customer engagement.
- Transparency and accuracy of claims**.**
- Records of processing activities.
- Categories of data to be processed.
- Incident and data breach management.
- Data protection officer / training.
- Data transfers.
- Registration.
- Sub-processors.

These modules help the data processor / sub-processor comply with articles within Chapter 4 of the UK GDPR and the UK Data Protection Act 2018.

Essential

Ref	Criteria
2.1.1	Applicants shall have a documented customer engagement process with version controls on all documents used.
2.1.2	A contract or other legally binding agreement shall be in place between the applicant and their customer which is compliant with Article 28 (3) of the UK GDPR and meets current UK Information Commissioner's Office guidance[1] Contracts shall set out: • The subject matter and duration of the processing. • The nature and purpose of the processing. • The type of personal data and categories of data subject. • The controller's obligations and rights. Contracts shall also include specific terms or clauses regarding: • Processing only on the controller's documented instructions. • The duty of confidence. • Appropriate security measures. • Using sub-processors. • Data subjects' rights. • Assisting the controller. • End-of-contract provisions. • Audits and inspections. Contract shall include details of the service being provided and include as a minimum: • Confirmation of agreed auditing detail. • Confirmation of agreed sanitisation process by media type. • Confirmation of agreement for logistical services to include hub usage and permission for multi-point collections if used during service provision. • Confirmation that the service issuer is the owner of the equipment and that they are legally entitled to release the equipment. • Confirmation of the point within the process where the applicant accepts custody of the assets. • Designation of the applicant as a data processor or sub-processor. • Agreement for the use of any third parties / sub-processors.

Guidance Notes

2.1.1 A documented process could be an illustrated workflow detailing the titles and version numbers of documents used.

2.1.2 [1] Current ICO guidance on contract can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Applicable UK GDPR Articles

Article 28 (3) It is a requirement for the processing activities to be governed by means of a contract.

Essential

Ref	Criteria
2.2.1	Website claims are reviewed and shall contain only accurate and true statements regarding processing activities.
2.2.2	Marketing material and customer contracts (2.1.2) shall contain only accurate and true statements regarding processing activities. All statements must be clear and unambiguous.
2.2.3	Applicants shall have a privacy policy on their website which conforms with UK Information Commissioner's guidance.[1]

Guidance Notes

ADISA assesses each certified company's website and reviews claims made about the applicant's service. This is done remotely at the same time as every audit whether this might be a full audit or a surveillance audit.

[1] Guidance on what should be included in a privacy notes is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/#what2

Applicable UK GDPR Articles

Article 5 (1) a This requires the processing of personal data is be done in a transparent manner. This criterion enables the customer to have confidence that the ITAD they are using is displaying in a public domain, correct claims about the processing activities.
Article 28 When selecting a processor, it would be fair for a controller to base part of that decision on claims made by the processor. In this regard claims made by the processor could be viewed by the controller as sufficient guarantees to conduct business with them.

Essential

Ref	Criteria
2.3.1	Applicant shall maintain a Record of Processing Activities (ROPA)[1] carried out on behalf of a customer. This shall be a written record and shall contain: • Name and Contact Details of the applicant and of each customer on behalf of which the processing activities are being carried out for. • Details where applicable of the Data Protection Officer. • Categories of processing carried out on behalf of each customer. • Where applicable detail of transfers to any third country. • Where possible a general description of the technical and organisational security measures which could include reference to appropriate policies and certifications held.
2.3.2	Where processing is carried out on behalf of a Competent Authority[2] and the processing activity is for the primary purpose of law enforcement, the ROPA shall also include a record of the lawful basis[3] for the processing activities being undertaken.

Guidance Notes

Whilst it is recommended to use the Information Commissioner's Office template[1] for the creation of the ROPA, a suitable format which the applicant has created is also acceptable.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how5

[2] A competent authority is defined in Schedule 7 of the DPA 2018. Data Protection Act 2018 (Schedule 7)

[3] Law enforcement purposes are defined under Part 3 of the DPA 2018. Data Protection Act 2018 (Part 3)

Applicable UK GDPR Articles

Article 30 (2) This requires the data processor to maintain a ROPA.

Essential

Ref	Criteria
2.4.1	Applicants shall have a documented security incident response procedure. This shall include: • Definition[1] of an incident including severity[2]. • Definition of what constitutes a data breach[1]. • Incident Response including disclosure[3] plan to customer[4]. • Incident investigation template including root cause analysis.
2.4.2	Applicants shall co-operate on request, with the ICO in the performance of its tasks.

Guidance Notes

[1] Align definitions with those laid out within Article 4 of the UK GDPR.
[2] Severity of events which occur within general business operations should clearly state when an event becomes classed as an incident which requires logging and investigating. Applicant should review the ICO's guidance on "breaches and near misses". Detecting, managing and recording incidents and breaches | ICO
[3] Disclosure plans should include clear timelines for reporting to the customer without undue delay (Article 33 (2)) and provide details of the reporting mechanism include any templates used.
[4] This scope of this Standard does not extend to situations where the applicants is acting as a data controller and so disclosure is only required in their role as data processor. The incident response plan could include disclosure to ICO and Data Subjects in the situation where the applicant is the data controller.

Applicable UK GDPR Articles

Article 33 (2) This requires the data processor to inform the data controller of a data breach without undue delay. This criterion assesses the procedure the data processor has in place to firstly identify events with a hierarchy of events such that a breach could be determined. At that point, this criterion assesses what their reporting process is to ensure that the data controller is indeed informed without undue delay.

Leadership and Oversight

Essential

Ref	Criteria
2.5.1	Applicants shall have a data protection policy which includes how all business operations ensure data protection requirements are met at all times. This shall include a requirement for ensuring staff are made aware of such a policy and are assessed on their understanding of the policy based on the requirements of their role.
2.5.2	Applicants shall have a documented organisational structure for managing data protection and information governance, which provides strong leadership, clear reporting lines and responsibilities, and effective information flows. Where a Data Protection Officer is not appointed, there should be a person of appropriate seniority designated as having responsibility for, and oversight of, data protection.
2.5.3	There shall be an internal audit programme to ensure compliance to this Standard is maintained and compliance to the data protection policy is assessed and confirmed on an ongoing and regular basis.
2.5.4	There shall be a regular assessment of technical and organisational measures which the applicant has in place to ensure their continued effectiveness.

Guidance Notes

2.5.1 A data protection policy should include policies and procedures for ensuring business operations are conducted in accordance with the overarching data protection policy.

2.5.2 Examples for how this can be achieved can be found in the ICO Accountability Framework.

Data Protection Officer

Essential

Ref	Criteria
2.5.5	Applicants shall carry out an assessment[1] regarding the appointment of a Data Protection Officer and document the decision. Where a DPO is appointed, the applicant shall register their details with the ICO.
2.5.6	Where a DPO is appointed the role and tasks of the DPO shall meet the requirements laid out in Article 38 and 39.

Guidance Notes

[1] Does my organisation need a data protection officer (DPO)? | ICO

A DPO can be an internal or external appointment but must meet the requirements must meet Article 37, 38 and 39 of the UK GDPR.

Applicable UK GDPR Articles

Article 37 (1) This requires the data controller and data processor to appoint a data protection officer where they are processing large scales of special category data.
Article 38 (2) This requires the data controller and data processor to provide appropriate resources to the DPO to carry out their tasks including the ability to maintain his or her expert knowledge.

Staff Training

Essential

Ref	Criteria
2.5.7	Applicants shall carry out a training needs analysis to assess what data protection training is required by each of the roles within their organisation. Each member of staff shall receive training aligned to their specific role.
2.5.8	Each employee shall undergo data protection training that has been signed off by a person of appropriate seniority designated as having responsibility for, and oversight of, data protection or the DPO if appointed, as part of their induction and before they start work associated with the data processing activities.
2.5.9	Each employee shall undertake annual data protection refresher training unless a training needs analysis has been carried out indicating a different frequency. Any such analysis must be documented, recorded, and signed off by a person of appropriate seniority designated as having responsibility for, and oversight of, data protection or the DPO if appointed.

2.5.10	For any staff member who operates machines or systems which perform a data sanitisation process, they shall have training prior to use and shall have refresher training done every year of service.
2.5.11	Applicants shall have a records of data protection training undertaken by each employee and evidence of follow up where training needs have not been met. As a minimum, these records shall be retained throughout the period of employment.
2.5.12	Applicants shall undertake an annual assessment of effectiveness[2] of the training programme. This assessment is to be undertaken by a person of appropriate seniority designated as having responsibility for, and oversight of, data protection or the DPO if appointed.

Guidance Notes

[1] Guidance on training programmes can be found on the ICO's website here: Training and awareness | ICO
[2] An assessment of effectiveness is to include an assessment of the employee's knowledge of data protection requirements in their role and also an assessment of the training programme which is in place to impart that knowledge on employees.

Essential

Ref	Criteria
2.6.1	Applicants shall not transfer data or move the physical asset prior to sanitisation, outside of the United Kingdom.

Guidance Notes

None.

Applicable UK GDPR Articles

Article 45 and 46 Whilst it is not expected for the ITAD being certified to this Standard to move physical assets across international borders, this criterion makes it explicit that this would not be permitted.

Essential

Ref	Criteria
2.7.1	Applicant shall undertake the ICO's self assessment[1] to understand if they are required to register with the ICO. When required they shall register with the ICO and pay the data protection fee unless they are exempt[2].

Guidance Notes

[1] Registration self-assessment | ICO
[2] https://ico.org.uk/for-organisations/data-protection-fee/

Applicable UK GDPR Articles

Whilst registration with the ICO is not mandated within the UK GDPR it is a requirement under the UK Data Protection Act 2018 for UK data controllers to register with the ICO.

Essential

Ref	Criteria
2.8.1	Applicants shall complete the sub-processor disclosure form and revalidate and submit to ADISA every six months.
2.8.2	The use of a sub-processor shall be disclosed to and approved in writing by the customer prior to work being carried out.
2.8.3	When a sub-processor is changed or new sub-processor appointed, the applicant shall disclose the change to the customer prior to the change occurring in order to permit the customer to object.

Guidance Notes

A sub-processor is a company who performs part of the data processing activities on behalf of the applicant. This does NOT include logistics or waste management but would include companies providing on-site shredding or hard drive repair services.

2.8.1 ADISA will make a request on all certified companies for an updated sub-processor disclosure form every six months.

2.8.2 Whilst it is recommended for this disclosure to be included within the customer engagement process an alternative means of disclosure can be presented and will be assessed on its own merits.

Applicable UK GDPR Articles

Article 28 (2) Data processors shall not engage another data processor without prior specific or general written authorisation of the data controller.
Article 28 (2) Data processors shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Essential

Ref	Criteria
2.9.1	Sub-processors shall be controlled by a contract which has the same explicit data protection obligations which the applicant has agreed with the customer. This is to include all aspects in 2.1.2.
2.9.2	Any sub-processor used to perform any part of the data processing service shall be audited by the applicant to ensure conformance with ADISA Standard. This can be done by a third-party or by the applicant but shall involve a physical audit and result in a written record. Self-validation by the sub-processor is not permitted.

Highly Desirable

Ref	Criteria
2.9.3	Any sub-processor used to perform any part of the data processing service should be ADISA certified.

Guidance Notes

2.9.1 The one variation on this might be the service level agreement (SLA) to perform the data sanitisation process. If an SLA is put in place with the data controller and the asset is not shipped to the sub-processor directly then the SLA agreement in place with the sub-processor should include the time the data processor has spent handling the asset.

For example, SLA to the data controller is 20 days to perform data sanitisation. The applicant collects equipment and holds for 5 days before shipping to sub-processor. In this case the SLA to the sub-processor should be lower that the hold time to ensure the data controller SLA is achieved so in this example the SLA would be 15 days to perform data sanitisation.

Applicable UK GDPR Articles

Article 28 (4) Data processors shall impose the same data protection obligations on any sub-processor which they have in place with the data controller.

The applicant may not provide data sanitisation services directly to a data controller but may be used as a sub-processor for another data processor. In these situations, the applicant shall comply with this module.

Essential

Ref	Criteria
2.10.1	Where applicant operates as a sub-processor, they shall record how they inform the data processor of the obligations under Article 28(4) that the data processor must put in place the same data protection obligations with the sub-processor as set out in their own engagement with their customer.

Guidance Notes

If the applicant processes data on behalf of another data processor then they are acting as a sub-processor. Under Article 28 (4) the same data protection obligations shall be applied to the sub-processor as are set out in the contract or other legal act between the data controller and data processor. Whilst not mandated the completion of the ADISA Acting as a Sub-Processor form would assist in compliance with this requirement.

Applicable UK GDPR Articles

Article 28 (4) Data Processors shall impose the same data protection obligations on any sub-processor which they have in place with the data controller. As the applicant may be operating as a sub-processor the form allows the auditor to capture evidence that the data processor has been made aware of their own obligations under Article 28 and that the applicant is permitted to act as a sub-processor on their behalf.

ICT Asset Recovery Standard 8.0

Section 3

Risk Management

Section Introduction

The business process of IT asset recovery typically involves a physical movement of the asset containing the data bearing media from a customer location to a data processing facility or to a location within the customer's own estate where the processing activity, data sanitisation, can take place. This physical movement has many areas of risk to the physical asset and a failure to mitigate through suitable countermeasures could make that risk too great to protect the rights and freedoms of the data subject.

This section assesses the IT asset recovery process and identifies where risk might exist and what countermeasures are in place to mitigate that risk. Mandated requirements are listed as Essential with Highly Desirable criteria not being mandatory but affording the applicant the opportunity to show enhanced capability. To enable the data controller to influence the required countermeasures a specific metric is introduced called the Data Impact Assurance Level (DIAL). The DIAL number is a measure of the data controller's own risk appetite and threat profile and includes the volume and categories of data being processed. This enables risk to be countered at a level which is commensurate to the data controller's own requirements. The DIAL concept is explained in Part 1 ADISA Asset Recovery Standard 8.0 – Introduction and Explanatory Notes.

Section 3 Core Principles

- Identification of Data Impact Assurance Level.
- Logistics.
- Processing Facility Capability.
- Data Sanitisation.
- On-site Services.

Applicable UK GDPR Articles

Within this entire section there are repeating requirements under the UK GDPR assessed within each module. For each article listed here they should be considered as being applicable throughout Section 3.

Article 24(1) This requires the data controller to take appropriate technical and organisational measures to ensure processing is undertaken in accordance with UK GDPR. To determine what is appropriate within the business process under evaluation, the DIAL rating is introduced to allow the data controller to provide the processor with a clear specification of the processes which are to be followed based on the metrics outlined in Part 1 Section 8.0. Within this section the risk posed to the physical asset when it is being moved outside of the security controls of the data controller are assessed to ensure these articles are complied with.
Article 5 (f) This requires the data controller to ensure appropriate security of the personal data is maintained which by means of this Standard allows that to happen.
Article 28 (1) This requires the data controller to only use data processors providing sufficient guarantees to implement appropriate technical and organisational measures.
Article 28 (4) Sub-processors are required to have the same data protection obligations so should comply with appropriate aspects of this section to evidence that.
Article 32 (1) b This requires the data controller to take appropriate technical and organisational measures to ensure processing activities are undertaken to ensure the ongoing confidentiality and integrity of personal data.
Article 32 (1) d This requires the data controller to have a process for evaluating technical and organisational measures which by means of this Standard allows that to happen.
Article 32 (2) This requires an assessment of the appropriate level of security based on the risks posed by the processing activities which by means of this Standard allows that to happen.

Essential

Ref	Criteria
3.1.1	Applicants shall identify the data controller DIAL reference and confirm it to be valid. Where applicant is operating as a sub-processor the data processor is required to provide this.
3.1.2	Applicants shall provide in writing to the data controller or, where acting as a sub-processor, to the data processor, confirmation of their own DIAL certificate issued as part of ADISA certification.

Guidance Notes

3.1.1 As part of becoming ADISA certified, each applicant will have their own micro-page on the ADISA website which they can use to enable the data controller to complete the DIAL assessment. This webpage will then email the data controller, the applicant and ADISA with a certificate bearing a unique reference ensuring all parties have the required information. Within this process the data controller will need to determine if the DIAL is for a specific collection, a project, a location or whether it can be applied company wide. They can also determine a validity period for the DIAL. The data controller also has the options to complete the same form on a non-ITAD specific page on the ADISA website but in this instance just the data controller and ADISA will be emailed copies of the certificate. Where the applicant is operating as a sub-processor the data processor shall be responsible for asking their customers to generate a DIAL reference by using the applicant's own micro-page.
To be classified as a "valid DIAL" one or more of the emails being entered onto the webpage shall have a data controller domain associated with it.

3.1.2 As part of the ADISA certification, each applicant will have a unique certificate issued to them which will confirm the DIAL rating they have achieved at audit as well as their overall certification award. This can be provided to the data controller or data processor within the contract, via email or some other means which creates an audit trail of this activity which excludes verbal communication.

A key risk during transportation is the exposure of assets during the movement from the location where they are stored to the vehicle to be used during transportation. This section assesses how factors which can increase that risk are identified during the engagement process so that operational processes can be applied to mitigate those risks.

<table>
<tr><th colspan="3">Identified Risk – Site Access</th></tr>
<tr><td colspan="3">Vehicle is unable to gain easy access to the site meaning it is parked further away than is necessary resulting in data carrying assets being moved outside of a secure perimeter.</td></tr>
<tr><th colspan="3">Risk Treatment (Criterion)</th></tr>
<tr><th colspan="3">DIAL</th></tr>
<tr><th>1</th><th>2</th><th>3</th></tr>
<tr><th>3.2.1</th><th>3.2.2</th><th>3.2.3</th></tr>
<tr><td>Site access details for each pickup location shall be captured in writing and communicated to relevant logistics staff / partners and shall include:

• Details regarding site access such as Parking Issues and any vehicle height restrictions.
• Confirmation of site security requirements such as vehicle driver identification requirements.</td><td>In addition to 3.2.1:

• Parking location identified and assessment of proximity to site made.
• Any other obstructions such as irregular activities including road works or public events requested.</td><td>Applicants shall perform a formal site survey using templates and following a written methodology prior to collection. Formal Site Survey shall include all details within 3.2.1 and 3.2.2.</td></tr>
</table>

Guidance Notes

3.2.1 and 3.2.2 Site access details can be captured in several ways including verbal (telephone) but should be recorded in a formal way such as on a system or specific form. Once captured this information should be shared with logistics staff or partners in a way so that a clear audit trail is created. Where there are no specific site access details for the job there should still be an audit trail confirming that there are no considerations required for that specific site. Site access only needs to be captured once but should be shared each time the site is being collected from. It is recommended that when sites are collected from regularly that site access is periodically checked and confirmed either by questioning the site contact or by asking for feedback from drivers attending site.

Guidance Notes (Continued)

3.2.3 This survey can be undertaken on-site or remotely but should follow a prescriptive method involving a written assessment of any practical aspect which could impact on the success of the collection.

Identified Risk – Building Access		
Asset location within the building where the collection is due to take place could hinder the collection process which might lead to assets being left unattended or increase the length of time the vehicle is left unattended.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.4	**3.2.5**	**3.2.6**
Building access details for each pickup location shall be captured in writing and communicated to relevant logistics staff / partners and shall include: • Location of items to be collected and details of any stairs or any other building feature that could inhibit collection. • Details of any oversized or heavy items including UPS and racks to be collected.	In addition to 3.2.4: • Detailed Inventory list to confirm type and volume of items for pick up. • Building access route identified and any issues noted. (For example, door height or width.)	Applicants shall perform a formal site survey using templates and following a written methodology prior to collection. Formal Site Survey shall include all details within 3.2.4 and 3.2.5.

Guidance Notes

3.2.4 and 3.2.5 Building access details can be captured in several ways including verbal (telephone) but should be recorded in a formal way such as on a system or specific form. Once captured this information should be shared with logistics staff or partners in a way such that a clear audit trail is created. Where there are no specific building access details for the job there should still be an audit trail confirming that there are no considerations required for that specific building. Building access only needs to be captured once but should be shared each time the site is being collected from.

3.2.6 This survey can be undertaken on-site or remotely but should follow a prescriptive method involving a written assessment and include requirements of 3.2.3.

It is often a commercial or geographic reality that the need for hubbing or staging of consignments is required. This is where the assets are stored at a different location whilst on route to the processing facility. These locations are identified as potentially high risk and this section assesses how this risk is disclosed to the customer to permit them to object and if allowed, how the applicant manages that risk to an acceptable level.

NB: The use of hubs shall be disclosed to and agreed by the customer as per 2.1.3.
NB: If the applicant does not use hubs then this section is scored as "not applicable".

Essential

Ref	Criteria
3.2.7	Hub locations shall be identified and disclosed during audit process. Where this is not possible, the applicant's customer engagement process shall include the customer's approval via clear written consent to the use of unidentified hubs during the logistics process.
3.2.8	Applicants shall ensure that hubs have suitable policies, procedures, and certifications in place to demonstrate that they understand their data protection/security obligations.

Guidance Notes

3.2.7 The only likely scenario where hubs cannot be disclosed is when networking logistics are used. This is a process where a logistics partner is used who sub-contracts the work out to a range of partners who in turn trunk the consignment in several locations where it moves from one logistics provider to another. This is common where movement over long distance is required so is an infrequent process within the United Kingdom.

3.2.8 Evidence of this will be determined by the applicant during their risk assessment / audit of the hub location. It would be expected to include vetting of staff, CCTV and alarms and processing in place to maintain the integrity of the physical perimeter and the consignment itself.

Identified Risk – Use of Hubs		
Exposure of physical asset when stored at an interim location enroute to the final processing facility (Hub).		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.9	**3.2.10**	**3.2.11**
Where multiple companies operate within the hub, each operator shall have a segregated operation from the other. Examples of segregation could be a cage, wall or any other physical barrier which precludes easy access to stored equipment. Where third party hubs are used, consignments shall not undergo re-packaging or re-palletisation.	Hubs shall be operated by one company. Where third party hubs are used, consignments shall not undergo re-packaging or re-palletisation.	In addition to 3.2.10, hubs are not used without prior written consent from customer.

Guidance Notes

3.2.9 and 3.2.10 Re-palletisation can only be undertaken if the load is unsafe or unstable. In this situation the applicant should control how this is to be undertaken within the contractual agreement with the hub operator / logistics partner.

3.2.10 An example of this would be where the hub is operated by the logistics operator. Where the hub is not operated by the logistics operator then the terms within 3.2.9 shall apply.

3.2.11 This can be achieved as per the requirement in 2.1.3 or in another formal way which creates an audit trail.

Identified Risk – Use of Hubs		
Exposure of physical asset when stored at an interim location enroute to the final processing facility (Hub).		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.12	**3.2.13**	**3.2.14**
Physical Hub Security shall include, but not be limited to: • Secure outer perimeter. • CCTV on all access points. • Alarm on all pedestrian and vehicle points. • PIR sensors in place to detect motion should physical perimeter be compromised.	In addition to 3.2.12, Storage Security shall include, but not be limited to: • Assets to be unloaded and stored under CCTV coverage. • Access Control shall be in place to ensure areas where assets are stored can only be accessed by authorised personal.	In addition to 3.2.12 and 3.2.13, hubs are not used without prior written consent from the customer.

Guidance Notes

3.2.12 and 3.2.13 This should be assessed as part of a formal audit of the hub which can be undertaken by the applicant or designated independent third party. This audit should include evidence of the assessment which could include a site plan and / or photographs.

Identified Risk – Use of Hubs		
Exposure of physical asset when stored at an interim location en route to the final processing facility (Hub).		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.15	**3.2.16**	**3.2.17**
Where hubs are used, consignment shall be signed into hub and then signed out of hub.	Chain of Custody shall be achieved by: • Consignment being booked in using a consignment box count which is to be verified during receipt. • Consignment is to be booked out using a consignment box count which is to be verified during exit.	In addition to 3.2.16, hubs shall not be used without prior written consent from the customer.

Guidance Notes

3.2.15 A consignment booking in is where the person receiving confirms receipt of the consignment as a whole and checks the integrity of packaging materials to assess whether tampering might be possible. An example might be a document which confirms that Job 1234 was received at the hub and was checked.

3.2.16 A consignment box count booking in, is a validation of the quantity of storage containers on the consignment. An example might be a document which confirms that 1 pallet or 3 boxes were received and signed into the hub and then signed out to the driver ahead of the return journey to the data processing facility.

3.2.17 This can be achieved as per the requirement in 2.1.3 or in another formal way which creates an audit trail.

Essential

Ref	Criteria
3.2.18	A fleet list shall be provided to ADISA of vehicles operated directly by the applicant and are used for asset recovery services. Any changes to this fleet require the applicant to notify ADISA within 30 working days of implementation.
3.2.19	Where any third-party vehicles are used by the applicant, for example short term rentals, there shall be written evidence of their conformity with the criteria within this module. This shall include details for how the vehicle will be GPS tracked during customer collections.
3.2.20	All records of collections made (which include relevant signatures) shall be retained by the applicant (digital or paper) for seven years.
3.2.21	Customers shall have the option to have collections made using vehicles with generic livery (i.e. non-task specific).
3.2.22	All vehicles shall be able to communicate with base via telephone or radio.
3.2.23	A full method statement shall be provided to include, but not be limited to: • Policy for comfort stops. • Policy for refuelling stops. • Policy for breakdown. • Plan for dealing with over and out of hours' situations.
3.2.24	Each driver shall have their driving licence or permit checked annually and details kept on their record.
3.2.25	Each driver shall have ID available for every collection.
3.2.26	The collection paperwork shall include named individual authorised to release the assets on behalf of customer.

Highly Desirable

Ref	Criteria
3.2.27	Each driver should have their driver licence or permit checked every six months.

Guidance Notes

3.2.18 Template for Fleet List submission available from ADISA.

3.2.19 Written evidence could be completion of Third-Party Confirmation Form or via a written agreement between applicant and third-party.

Guidance Notes (Continued)

3.2.20 Generic livery would be viewed as any livery which is non-task specific. An example might be “ACME Logistics” whereas “ACME Computer Recycling” is not. In instances where applicant has their fleet liveried and it is task specific, within the customer engagement process there should be clear options for the customer to request vehicles with generic livery.

3.2.21 Applicant should be able to prove ability to provide generic liveried vehicles which could be via an agreement in place with a rental provider or third-party logistics provider.

3.2.22 Where third parties are used this requirement is expected to be included within the terms of service or contract in place with the logistics service provider.

3.2.23 Where third parties are used this document should be held on file by the applicant and made available to ADISA during the audit process.

3.2.24 Where third parties are used this is expected to be included within the terms of service or contract in place with the logistics service provider and will be confirmed during the applicant’s audit of the third party.

3.2.25 Where third parties are used this is expected to be included within the terms of service or contract in place.

Identified Risk – Exposure during transportation		
The vehicle when it is in transit might be compromised with loss of the physical asset.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.28	**3.2.29**	**3.2.30**
Each vehicle shall be able to communicate with base via telephone or radio.	In addition to 3.2.28, each vehicle shall have suitable physical protection such as electronic or mechanical immobiliser and/or an alarm. Each vehicle shall be solid sided and have solid bulkheads.	In addition to 3.2.29, each vehicle shall have additional locking security such as slam locks or isolated tail-lifts.

Guidance Notes

3.2.29 A bulkhead is the part of the vehicle between the cab and the load carrying area.

Identified Risk – Exposure during transportation		
During the logistics process the vehicle is compromised and taken off route to permit access to the load either by an insider (driver) or external threat adversary.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.31	**3.2.32**	**3.2.33**
Each vehicle shall be GPS tracked which shall allow for: • Historical data to be stored for a minimum of six months. • Route history to be available upon request. All drivers must be informed that their vehicles movements are being tracked via GPS to comply with UK GDPR.	In addition to 3.2.31, each vehicle shall be GPS tracked and have stationary alert enabled. There shall be a process for reviewing such alerts with a response plan in place.	In addition to 3.2.32, each vehicle shall be GPS tracked with a Geo-Fencing Route in place. Or Each Vehicle is to be escorted by the customer.

Guidance Notes

3.2.31 This countermeasure is a deterrent to the driver themselves as they know the GPS is in place and could be used to identify any unusual activity which might take place.

3.2.32 This is a reactive countermeasure which alerts base to any stationary activity and elicits a response from the applicant.

3.2.33 This countermeasure is a proactive control by predefining the route either via geo-fencing or escorting.

Identified Risk – Exposure during transportation		
Vehicle is left unattended during multi-point collections.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.34	**3.2.35**	**3.2.36**
Site Access information shall be captured as per 3.2.1.	In addition to 3.2.34, two operatives shall be sent on all collections with a written collection method statement which confirms the vehicle is not to be left unattended.	Direct back to facility collections shall be done**.**

Guidance Notes

3.2.36 A direct back to facility collection is when the vehicle goes directly to the facility from the collection point. This means no hubs are used. If the vehicle is performing multi-point collections, the final collection would be viewed as direct back to facility if the vehicle returns from that collection point to the facility.

Identified Risk – Exposure during transportation		
Load slips during multi-point collections so assignment of assets to different customers is compromised.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.37	**3.2.38**	**3.2.39**
Applicants shall ensure there is physical separation of loads which is sufficient to maintain segregation and to ensure no load slippage can mix consignments. Applicants shall ensure that each part of the load shall have a unique identifier able to identify the customer.	Multi-point collections from different customers shall include additional security countermeasures such as: • Lockable totes or crates. • Security tags on each consignment.	Serial number scanning or unique identifier scanning is undertaken on customer site.

Guidance Notes

3.2.37 There are many ways for the applicant to achieve this including the use of packaging and separators on the vehicle.

3.2.37 The unique identifier shall be a reference which can be directly tracked back to the customer who has booked the job.

3.2.38 Lockable totes or crates should be secured in such a way that assets cannot be removed. In this regard the physical dimensions of the asset might make one method invalid which was permitted for a different asset type. For example, smart phones or loose hard drives are significantly smaller than PCs so the use of cages with mesh which is wider than a phone would not be classed as meeting this requirement even if the cage was locked. The reason is that the asset could be removed from the collection material through the mesh.

3.2.39 The scanning process should be automated to avoid human error. For this reason, manual processes such as writing down of serial numbers would not be permitted.

Identified Risk – Third Party Contractor		
Use of a Third-Party logistics partner leads to variation from the required service which increases risk to the physical asset during the transportation process.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.2.40	**3.2.41**	**3.2.42**
Any third parties used to perform any part of the logistics service shall be controlled by means of a formal written contract, which includes confirmation that third-party vehicles and service meet all requirements of DIAL 1 requirements within this Module with specific reference to; • Staff vetting. • Documented security incident procedure. • Vehicle Specification.	There shall be a written collection process which includes a risk assessment that identifies and mitigates all clear risks to the integrity of the consignment. For example: Doors to be closed and locked whenever the vehicle is to be left unattended. This shall be included in the driver induction or handbook. Any third parties used to perform any part of the logistics service shall be audited **annually** by the applicant to ensure compliance with Section 3 Module 2. This can be done by a third-party or by the applicant but shall result in a written record and contain evidence. Self-validation by the logistics provider is not permitted.	Applicants shall operate its own fleet operated by its own staff. Occasional use of third parties for specific requirements or emergencies is permitted. OR Where a third party is used the applicant shall chaperone the collection or escort the vehicle.

Guidance Notes

None.

The control of the physical asset is crucial to ensure the data processing activities have taken place as prescribed by the customer on ALL target media. Throughout the process the asset management needs to be controlled and the transfer of custody from one entity to another clearly defined.

Essential

Ref	Criteria
3.2.43	The collection paperwork shall include: • A signature, printed name, and date shall be obtained from the releasing person or agent on behalf of the customer. • A signature, printed name and date, shall be obtained from the logistics representative. • A signature, printed name and date, shall be obtained from the receiving employee at the processing facility.

Guidance Notes

None.

Identified Risk – Loss of Asset		
Loss of asset from point of release from the customer to the point when data sanitisation takes place.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.1	**3.3.2**	**3.3.3**
Chain of custody shall be achieved by identifying a count of boxes / pallets / containers in the consignment. This count shall be verified and signed for by the customer and recipient before leaving site.	Chain of custody shall be achieved by identifying a count of assets by type on site. This count shall be verified and signed for by the customer and recipient before leaving site.	Chain of custody shall be achieved by identifying a count using a unique reference identifier such as a serial number. This count shall be verified and signed for by the customer and recipient before leaving site. This capability shall include verification on receipt at the facility and at the end of the process itself.

Guidance Notes

3.3.1 An example of this would be a collection which was verified by confirming the number of sealed boxes received.

3.3.2 An example of this would be a collection which was verified by confirming the number of asset types (e.g. 20 x PC) which were received.

3.3.3 This is where asset management is done on unique identifiers. This could be done by manually checking off against pre-printed lists OR by creating the list on site by scanning serial numbers. Provision should be made for dealing with devices which do not have serial numbers, or which would not scan.

Identified Risk – Asset Management		
Applicant or their appointed partner loses an asset during the collection process.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.4	**3.3.5**	**3.3.6**
Every collection to be processed shall be individually tracked within **72 hours** of receipt at the facility unless expressly written into a contractual service level agreement (SLA) for customer specific requests.	Every collection to be processed shall be individually tracked within **24 hours** of receipt at the facility unless expressly written into a contractual SLA for customer specific requests.	Every asset to be processed shall be individually tracked from **point of collection**.

Guidance Notes

3.3.4 and 3.3.5 Individually tracked means every asset is booked in using a unique identifier such as serial number or barcode.

3.3.6 Typically this would be achieved by onsite scanning to create the inventory although other ways are possible such as the use of pre-printed barcodes, stickers or third-party verification tags.

Identified Risk – Unexpected Assets Found		
Items are found at the processing facility which were not identified during the collection process.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.7	**3.3.8**	**3.3.9**
Upon receipt at the facility any loose or separate data carrying product or media including tape which were not listed on the inventory shall be individually tracked on the system and classified as a separate asset.	Upon receipt at the facility any loose or separate data carrying product or media including tape which were not listed on the inventory shall be individually tracked on the system but quarantined before being processed and disclosed back to the customer to await direction. They should be identified as being in quarantine on the system and held in a clearly marked segregated area.	Upon receipt at the facility any loose or separate data carrying product or media including tape which were not listed on the inventory shall be quarantined as per 3.3.8 but raised as an incident and investigated accordingly as per 2.4.1. They should be identified as being in quarantine on the system and held in a clearly marked segregated area within the security-controlled environment.

Guidance Notes

3.3.7 Once booked onto the system these assets should be processed in accordance with the contracted terms based on their media type.

3.3.8 The applicant should have a quarantine policy which controls the process once the asset is identified as requiring quarantine. This should include determination of who within the applicant is responsible for managing the process and what timelines are in place. The applicant should consider putting the policy within the contract so that all parties understand their roles and the timelines to resolution.

3.3.9 This follows the same process as 3.3.8 but is raised as an incident and the incident response process enacted. As per the definition within UK GDPR Article 4 (12), unauthorised processing could be determined as data breach and the incident response process will enable the applicant to assess why additional assets were released without being controlled so that they can determine whether there is a process failure and identify remediation required.

Section 3 Module 3 Processing Facility Capability – Physical Security

ADISA Certification requires that all aspects of the applicant's site shall be secured to deter either opportunist intruders or determined planned attacks. As such both physical and technological deterrents are needed to provide a layered approach to physical.

Essential

Ref	Criteria
3.3.10	Where CCTV is in operation there shall be visible and legible warnings that CCTV is in use in locations where it can collect images of employees or members of the public.
3.3.11	CCTV coverage shall be recoverable for at least one week. Recorder shall be protected from threat of theft, fire and technology failure.
3.3.12	Images recorded and recoverable from CCTV systems shall be fit for purpose and provide quality, usable footage of areas covered.
3.3.13	Perimeter walks shall be carried out weekly and documented to confirm checks are made on: • Buildings in the vicinity to check for change of use or vacant lots. • Position and line of site of all external cameras. • Perimeter fencing (if in place) to check for signs of damage.

Guidance Notes

3.3.10 In addition to the signage the applicant should undertake the Information Commissioner's Office CCTV check list. https://ico.org.uk/for-organisations/data-protection-self-assessment/cctv-checklist/

3.3.11 Applicant should assess whether their current CCTV recording, and storage process could be compromised by theft, fire or technology failure and, if such a compromise is possible, to put in place additional countermeasures to reduce that compromise. For example, if the DVR does not have any resiliency (such as running RAID or being mirrored) then a backup process would protect from technology failure.

3.3.13 A perimeter walk should be carried out by an appointed and trained member of staff who has guidance on what to look for and how to determine if a change is worth investigating. All perimeter walks should be logged.

Section 3 Module 3 Processing Facility Capability – Physical Security

Identified Risk – Theft by break in		
Facility physical perimeter could be compromised.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.14	**3.3.15**	**3.3.16**
The facility shall have a solid physical perimeter which creates a barrier to entry for unauthorised access.	The facility shall have two layers of physical security.	The facility shall have the ability to process customer assets within a third layer of physical security if required to do so.

Guidance Notes

3.3.14 A solid physical perimeter would be defined as a barrier sufficient to stop a threat adversary attempting to gain access using tools which are manually operated or mechanical tools which are defined as powered tools but excluding cutting tools.

3.3.15 A second layer of physical security could be an external perimeter fence around the facility or a cage controlling access within the facility should no external perimeter fence exists. The positioning of the facility regarding ease of access will also be considered, for example, on a trading estate which itself has perimeter controls and vehicle access controls. In addition, the data processing area location within the facility can also be considered as physical security if it is visually obscured from ease of access (such as on a mezzanine).

3.3.16 A third layer of security could be the provision of any two layers of physical security laid out in 3.3.15 in addition to the requirements of DIAL 1.

Section 3 Module 3 Processing Facility Capability – Physical Security

Identified Risk – Theft by break in		
Facility physical perimeter could be compromised.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.17	**3.3.18**	**3.3.19**
Facility shall have CCTV coverage in place which covers the following areas: • All pedestrian access points including fire exits. • Where the vehicles are unloaded to ensure vehicle registration is visible, and visibility of the loads is achieved. • Extensive coverage within the data processing area.	In addition to 3.3.17 the quality of the CCTV footage shall be good enough to permit the identification of individuals via facial details and / or vehicle registration details on the areas covered. The CCTV solution is also to have: • Footage which is to have time and date stamp and be synchronised regularly. • Location of external cameras is to be such that tampering by intruders or staff without equipment would be impossible.	In addition to 3.3.18, CCTV shall cover the following areas: • All external aspects to be covered. • Vehicle access points to site to be covered.

Guidance Notes

3.3.17 Suitable coverage would be able to identify the registration of the vehicle.

3.3.18 Facial details does NOT mean facial recognition software, only that the footage should be good enough to be able to identify the faces of people within the areas in question.

Section 3 Module 3 Processing Facility Capability – Physical Security

Identified Risk – Theft by break in		
Facility physical perimeter could be compromised.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.20	**3.3.21**	**3.3.22**
Applicant shall have an intruder alarm installed to recognised national standards. Facility shall have alarm points on all pedestrian and vehicle access points. In situations where the latter is not possible then PIR coverage is required.	In addition to 3.3.20, there shall be an alarm response plan which details how the alarm is monitored, what happens when it is triggered and evidence clear escalation process. Alarm Response plan shall be tested at least once per year with the results documented and remediation plan put in place for any matters arising from the test.	In addition to 3.3.21, the site shall have out of hours physical security coverage which can include alarm and camera monitoring or on-site security guards.

Guidance Notes

3.3.20 The alarm installation companies will be able to provide details of the Standards against which the installation was carried out. Examples of these might be PD6662:2004 or BS EN 50131-1:2004.

3.3.20 An example where an alarm break point might not be possible to utilise could be where a shutter is subject to significant wind. In this situation an alarm break point on the shutter might be falsely activated which over time will erode the response to alarm activations. ADISA would accept no alarm points on such doors but would expect to see internal PIR in place which would activate if the shutter were opened or otherwise compromised for example by a vehicle ramming.

3.3.21 An alarm response plan should include details of people involved, their roles and guidance on their actions.

3.3.22 Out of hours physical security coverage should be performed by external professional companies. They should either be on-site or operating remotely but able to actively monitor CCTV cameras.

Section 3 Module 3 Processing Facility Capability – Physical Security

Identified Risk – Theft by break in		
Intruder breaks through physical perimeter and is inside the building without being detected.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.23	**3.3.24**	**3.3.25**
Passive Infrared (PIR) sensors shall be in place to ensure that intrusion would be detected in all main areas of the data processing areas.	In addition to 3.3.23, PIR sensors shall have extended coverage such as on external walls, all windows and roof.	In addition to 3.3.24, facility shall have exterior fitted proximity lighting operating out of hours. Any obvious points of entry such as easily accessible windows or roof lights, shall have additional security countermeasures such as bars or alarms. Facility shall have smoke/fog or acoustic intruder system in the processing area.

Guidance Notes

3.3.23 The expectation is that if an intruder had gained entry to the main processing area that their presence would be detected by the PIR and activate the alarm.

3.3.24 The expectation is that if an intruder were to affect entry via one of these means then their presence would be detected by the PIR and activate the alarm.

3.3.25 These countermeasures are external such that attacks on the physical perimeter are being assessed prior to them being breached.

Section 3 Module 3 Processing Facility Capability – Physical Security

Identified Risk – Theft by break in		
The business activity undertaken at the premises is seen by an opportunist and increases the risk to the building becoming a target.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.26	**3.3.27**	**3.3.28**
Once unloaded, all equipment shall be taken inside the premises immediately.	In addition to 3.3.26, the facility shall show no external signs of the data processing activities undertaken at the site.	In addition to 3.3.27, vehicles shall be unloaded such that public cannot view unloading activity which can be achieved by unloading inside the facility or at the threshold of the facility.

Guidance Notes

3.3.26 The expectation here is that equipment being unloaded is within public view for the shortest possible time.

3.3.27 The expectation here is that the applicant does not attract interest in the activities within the facility by external signs of those activities. Examples might be obvious signage or the presence of a retail outlet on the premises.

Section 3 Module 3 Processing Facility Capability – Internal Security

One of the main security control challenges is mitigating the potential for insider theft. ADISA will audit internal security countermeasures, staff checks and controls that minimise the risk for potential insider theft.

Identified Risk – Insider Theft		
Access could be gained by entities operating legitimately within the physical perimeter.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.29	**3.3.30**	**3.3.31**
The premises shall not be shared with any other organisation without significant physical segregation and access controls to be in place.	The premises shall be operated and occupied solely by the company being certified.	The premises shall be operated and occupied solely by the company being certified.

Guidance Notes

For applicants which are part of a group of companies with the same ownership, then these will be viewed as one company if all employees are screened and managed in the same way as the applicant.

3.3.29 Significant physical segregation could be via walls, cages, or clear dedicated areas.

3.3.31 Is intentionally the same as 3.3.30.

Section 3 Module 3 Processing Facility Capability – Internal Security

Identified Risk – Insider Theft		
Access could be gained by employees who are not authorised.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.32	**3.3.33**	**3.3.34**
The premises shall not have any other business process operating out of the facility without significant physical segregation and same site security standards to be in place and verifiable.	The data processing facility shall have controlled access for authorised staff only.	In addition to 3.3.33, access control shall record which staff entered and exited the processing area.

Guidance Notes

3.3.32 Significant physical segregation could be via walls, cages, or clear dedicated areas.

3.3.33 There should be a clearly defined access perimeter to the data processing area. This could be controlled by mechanical digital door locks or other suitable means.

3.3.34 The record of access can be achieved by individually issued access cards which record usage or any other means but should result in a log which can be retained and reviewed for a period of at least 30 days.

Section 3 Module 3 Processing Facility Capability – Internal Security

Identified Risk – Insider Theft		
Theft of physical device or access to data by employees.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.35	**3.3.36**	**3.3.37**
Non-full-time staff (e.g., temporary or contract workers) shall not be used in data processing areas unless they have already undergone the same extensive screening as full-time staff or are chaperoned within data processing areas. All new starters who have access to data bearing assets shall have their vetting applied for on or before the start of their employment. During this time new starters who are not vetted shall be chaperoned until vetting has taken place.	In addition to 3.3.35, Insider theft shall be discouraged by a blend of physical and procedural checks. The following shall be used as part of this: • The use of staff lockers which shall be separate to the processing areas. • Restrictions on personal items being allowed within the processing area. • Any phones permitted must have IMEI numbers recorded and checked weekly. • Staff purchase schemes for stock items.	In addition to 3.3.36, random staff searches shall be in operation. Staff searches shall utilise electronic wands and / or body scanners.

Guidance Notes

3.3.35 If the vetting is not in place, then evidence would be required of the application for vetting to be carried out which should be before or on, the start of the employee's employment.

3.3.36 Where warehouses are cold there can be an exception for coats and jackets where there are staff searches in place. Where there are no searches in place then the applicant should make provision for other suitable workwear to be provided.

3.3.37 Staff searches should be undertaken by an identified member of staff, and they should be documented when and on whom the search took place.

Section 3 Module 3 Processing Facility Capability – Internal Security

Identified Risk – Insider Theft		
Theft of physical device or access to data by visitors.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.38	**3.3.39**	**3.3.40**
The general facility shall have controlled access which will include the following: • No visitors or unauthorised staff will be allowed into data processing areas unless they have their identification verified using photo ID and it is recorded. (NB: This includes drivers, tradesmen and office visitors.) • All visitors and unauthorised staff will always be escorted when in the data processing area.	In addition to 3.3.38, visitors shall wear clearly visible badges and / or vests, which identify them as being non-staff and are always to be escorted in processing areas.	Same as 3.3.39.

Guidance Notes

None

How assets are handled within the facility is critical to maintaining control and ensuring each asset undergoes the correct data sanitisation treatment.

Essential

Ref	Criteria
3.3.41	In the absence of a written customer specification, every asset shall be audited to obtain a full build specification and create an asset inventory with each asset being uniquely identified.
3.3.42	All equipment shall undergo de-branding where asset tags and other non-relevant markings are removed.
3.3.43	Each device shall have the chassis opened to check for unconnected data carrying media such as hard disk drives and full physical checks for other storage devices made (e.g., by opening CD drawers, searching any packaging / bags for removable media) and to identify any external storage such as memory cards which might be connected to the device / be included in the consignment. Any media found will be processed in accordance with this Standard.
3.3.44	Any customer engagements which require the holding of data carrying assets for longer than the recommended time period shall be managed by a written agreement by the applicant and the customer, which expressly states that the recommended time has been exceeded at the customer's wishes.

Guidance Notes

3.3.41 Typical build specification will include CPU, RAM and Storage.

3.3.42 Any marking which could be used to identify the original customer should be removed. This includes those which are etched.

3.3.43 This is not necessary on small form factor devices such as smart devices and laptops where additional media would be impossible to fit into the chassis / casing.

3.3.44 This is not part of the unexpected item quarantine process but a known and expected request from a customer to delay processing. This is often called a cooling off period and can occur upon receipt or after initial audit. In either case, this should be agreed in writing.

Identified Risk – Processing times		
Data Processing activity is longer than necessary.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.45	**3.3.46**	**3.3.47**
In the absence of a written customer specification the maximum length of time from the point of collection until the point of data sanitisation shall be done as soon as possible but no longer than **45 working days.**	In the absence of a written customer specification the maximum length of time from the point of collection until the point of data sanitisation shall be done as soon as possible but no longer than **20 working days.**	In the absence of a written customer specification the maximum length of time from the point of collection until the point of data sanitisation shall be done as soon as possible but no longer than **five working days.**

Guidance Notes

The time to data sanitisation is worked out from the date of collection through to when the media is actually sanitised. In this regard it includes any time spent at hubs and if a sub-processor is involved, the time it takes to ship to them and for them to process.

Section 3 Module 3 Processing Facility Capability - Segregation

This is how the applicant controls the physical asset such that assets which still have data on cannot be mixed with assets which have been data sanitised.

Identified Risk – Contamination of processing streams		
Pre (data carrying) and Post (data safe) assets might get mixed up within the processing facility.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.3.48	**3.3.49**	**3.3.50**
Data carrying equipment shall be **visually** segregated from post process equipment. Any opportunity for cross contamination of these assets needs to be marginalised, and where any exist managed appropriately.	Data carrying equipment shall be **physically** segregated from post process equipment. Any opportunity for cross contamination of these assets needs to be marginalised, and where any exist managed appropriately.	In addition to 3.3.49, processing shall be system managed with controls which stop an asset from being further processed until data sanitisation is confirmed**.**

Guidance Notes

3.3.48 Visual segregation includes the use of space or labelling to determine where the physical asset is in the process. This could be the use of stickers such as Red / Green or Data Unsafe / Data Safe or barcodes.

3.3.49 Physical segregation includes a process flow whereby assets are processed in a way such that the processing flow does not cross back on itself (Ideally processed in a linear fashion). In addition, the use of cages or walls or other physical barriers can provide for clear demarcation between assets being processed and those which are ready for sale.

3.3.50 System managed would be a processing management software which is used to control inventory. The system should include gateways between stages within the processing flows such that the asset on the system cannot progress, for example, to the sales stock, unless there has been a positive action on the system to confirm that the device is data safe. This would ideally be largely automated by integration with overwriting software but will also require manual input for media which is reset such as networking equipment or which fails an overwrite and is destroyed.

Records created during the processing of assets need to be safeguarded, so that in the event of a disaster or theft the records can be recovered, and customers can be assured that their data carrying assets were processed correctly.

Essential

Ref	Criteria
3.3.51	Processing system shall have functionality which allows its records to be interrogated and allows the recall of items by searching using a unique identifier which stays with the asset being processed.
3.3.52	Processing system shall be backed up weekly.
3.3.53	Back up shall be tested once a year.
3.3.54	Back up shall be stored off site or in a secure, fire retardant location on site.
3.3.55	Processing systems shall be configured such that they are checked for vulnerabilities and patched, as necessary.

Highly Desirable

Ref	Criteria
3.3.56	Processing system should be backed up daily.
3.3.57	Back up should be tested once a quarter.

Guidance Notes

3.3.51 A processing system is the software used to manage the service being undertaken. It should be able to track an asset using a unique identifier such as serial number back throughout each stage of the process allowing the identification of customer contract, collection notes and sanitisation activities performed. This can be more than one piece of software but navigation between the two should be clear.

A critical part of the compliance requirement of this business process is the ability for the data processor / sub-processor to report back to the data controller / data processor on the processing activities which have taken place. This section looks at what is required to be within the reporting outputs from this business process.

Essential

Ref	Criteria
3.3.58	The applicant shall provide the customer with detailed audit reports to include as a minimum, but not be limited to: • Serial numbers of devices. • Make. • Model. • Evidence of end point sanitisation.
3.3.59	Applicant reports shall include copies of the documents used to control the transfer and chain of custody (For example: Collection Notes and / or Waste Transfer Notes) from point of collection through to delivery into processing facility.
3.3.60	Applicants shall provide the customer with copies of certificates of destruction and any applicable waste compliance reports.

Highly Desirable

Ref	Criteria
3.3.61	In the absence of a specific written customer specification the applicant should provide the customer with detailed audit reports which should include: • Disk drive serial numbers. • Software overwriting report / reference numbers.

Guidance Notes

3.3.58 Evidence of end point sanitisation should include the inventory of the assets processed and the means of sanitisation.

3.3.59 The transfer of custody should show where the current custodian transfers custody to the next, for example customer to driver of a vehicle. The chain of custody should show how the inventory is transferred from one custodian to the next and how checks are made on that inventory. These could be one or more documents but must show the entire chain of custody.

Guidance Notes (Continued)

3.3.60 If the shipment has been designated as waste the applicant shall provide the waste producer with the necessary reports as per Environment Agency requirements.

3.3.61 Each software overwriting product used should generate a unique reference for the drives which are overwritten. These references should be cross referenced to the drive serial number.

These criteria are used to assess the way in which sanitisation tools are used within a data sanitisation production environment.

Essential

Ref	Criteria
3.4.1	Each applicant shall have all data sanitisation tools identified, verified, and published by ADISA in their Data Capability Statement. These tools must meet the minimum sanitisation requirements[1] laid out by ADISA.
3.4.2	Every data carrying device, which is received for data processing, shall undergo a data sanitisation process regardless of any assurances from the customer that they have already destroyed the data.
3.4.3	Any data carrying device which fails shall be removed from parent machine, individually tracked via a unique identifier and on-site physical destruction shall take place within a controlled and documented process.
3.4.4	Applicant shall confirm if the data controller wishes to follow a re-use or destruction process for data sanitisation.

Guidance Notes

3.4.1 Data Capability Statement can be presented in any format, but it is preferrable to use the ADISA template available. It should include as much information as possible including details of specification for any physical destruction. For example, for shredding it should include the shred particle size. For software overwriting it does not necessarily need to confirm a brand name for software but where it does the version number should be included. Where a brand name of software is not listed then the certifications held by the software should be listed. For example, CPA Approved Software.

[1]To understand what the minimum sanitisation requirements are please use the current ADISA Data Capability Requirements guidelines which can be found here at ADISA Data Capability Requirements.

3.4.2 Regardless of claims made by the customer that data has been removed, the applicant is to process media in the same way.

3.4.3 If a drive or other media / product fails to be software overwritten either due to a mechanical failure or due to the overwriting process to be incomplete, then the media should be individually tracked on the processing system such that it can be tracked back to the originating device and either undergo another attempt at wiping OR be physical destroyed as per the data capability statement. This physical destruction should take place on applicant premises.

3.4.4 This can be determined within the contract, via email or some other means which creates an audit trail and is essential to help the applicant understand whether the consignment is to be viewed as product for reuse or waste for recycling. It will also help the applicant determine how much time to apply to the asset to promote reuse as assessed within Section 4 Module 2. Where the applicant is working as a sub-processor the written confirmation from the data processor should be explicit when it confirms the intention of the data controller.

These criteria are used to assess the way in which sanitisation tools are used within an ITAD production environment.

Software Overwriting

Software overwriting is the use of a software to write data strings to the media to overwrite existing data and render it unrecoverable. The data strings written can vary depending on overwriting standards as can the number of times the entire accessible writable area of the media shall be written to.

Essential

Ref	Criteria
3.4.5	Software overwriting tools shall be configured in a known and documented configuration with monthly checks on the configuration to be carried out and documented by staff NOT directly involved in the software usage. Configuration shall include controls in place to deal with the following: • Identification of HPA and DCO. • Tolerance for remapped sectors. • Options for controlling verification. • Options for dealing with specific overwriting algorithms. • Options for determining number of times overwriting. • Documented means of checking for and receiving updates from software vendor.

Guidance Notes

3.4.5 Software overwriting tools in use should have functionality to control all these options. The applicant should have a documented approach to configuring the software to ensure it is in a known state. They should also have a change management process for how changes to the configuration are controlled, authorised, and confirmed. The users of the software cannot make changes without management sign off which should all be documented.

Any matters arising from the quality checks carried out as per 3.4.11 – 3.4.13 should be dealt with as an incident and the configuration of the software overwriting tools investigated with any mediation resulting in a change in the documented configuration.

Shredding

Shredding is the process where the media is presented to a specialist machine which has a set of teeth / blades designed to shred the device into pieces. Many shredders have screens beneath them to provide a crosscut as opposed to a strip cut. Each screen will have apertures matching the requested shred size to ensure the particulate can only pass through when reduced to the agreed standard.

Essential

Ref	Criteria
3.4.6	Any shredders which are used shall have a maintenance schedule (which is to include screen aperture assessment), be manufactured for use on the media and have a user training programme in place.
3.4.7	In the absence of a written customer specification, ALL shredders used shall have undergone independent verification of the maximum shred particle size which is to be published as per 3.4.1.
3.4.8	All shredders shall have hoppers / feeds checked after each period of usage to ensure all media have been shredded. Specific attention shall be made when shredding Solid State Drive or other flash-based media to ensure that there are no intact NAND cells within the hopper / feed or the shred particulate.

Guidance Notes

3.4.6 User training programme should include health and safety as well as operational guidance on the shredders use.

3.4.7 ADISA can measure this as part of the audit process. This assessment will use callipers to measure the screen aperture and the particulate size from the output of the shred.

3.4.8 This process should form part of the training for users of shredders. Any repeating issues should be viewed as an incident and acted upon as per 2.4.1.

Degaussing

Degaussers emit a magnetic field measured in units of Gauss or Oersteds (Oe) with the objective of removing the magnetic properties of the coating on the platter of magnetic hard drives or tape surface.

Essential

Ref	Criteria
3.4.9	In the absence of a customer specification, only degaussers from the NSA approved list[1] can be used. All degaussers used shall be properly calibrated, have a regular maintenance schedule and a user training programme in place which includes a process for removing all extraneous steel shielding materials (e.g., cabinets, casings, and mounting brackets), but not the hard disk assembly, shall be removed before degaussing.

Guidance Notes

3.4.9 The National Cyber Security Centre no longer approves degaussers for use within the UK and defers to the National Security Agency in the United States for product approvals. Applicant should review www.nsa.gov to find the current list[1].

[1]At time of release the current list of approved products dated July 2019 can be found here; https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/NSAEPLMagneticDegaussers%20June2019.pdf?ver=2019-07-03-090458-077

3.4.9 ADISA will test the magnetic field output from all degaussers used as part of the audit process and will assess against manufacturers claims to ensure they are operating within manufacturers guidelines.

Other physical

A physical deformation process designed to make the media non-functional.

Essential

Ref	Criteria
3.4.10	Any other physical deformation process such as folding, crushing or any other means which impairs the operation of the media, shall meet the minimum specification set out in the ADISA Data Capability Requirements[1].

Guidance Notes

3.4.10 There are many physical processes which can be applied to media to render the physical device inoperable. Where the process does not meet the minimum Data Capability Requirement set out by ADISA, a secondary sanitisation process shall be carried out which does meet these requirements.

[1] To understand what the minimum sanitisation requirements are please use the current ADISA Data Capability Requirements guidelines which can be found here at ADISA Data Capability Requirements.

Section 3 Module 4 Data Sanitisation – Quality Control/Verification

There are different data sanitisation techniques which can be utilised. Some visually impact the media such as shredding whereas others may not. It is essential for the applicant to ensure the data sanitisation technique has been successful by performing a quality control / verification check. The quality control check for shredding is covered in 3.4.8 and all other data sanitisation techniques shall comply with the following.

Identified Risk – Data Breach		
Media or device did not undergo an approved means of sanitisation.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.4.11	**3.4.12**	**3.4.13**
There shall be a documented quality control process, which will check a sample number of devices per month after the data sanitisation process has been complete. The minimum sample size shall be ten **per month** of all product types with a sampling log kept. Logs to be kept for a six-month period.	In addition to 3.4.11 but the minimum sample size shall be ten **per week** of all product types with a sampling log kept.	In addition to 3.4.12 but **EVERY** device shall be checked to ensure the sanitisation technique was applied to it.

Guidance Notes

3.4.11 and 3.4.12 A quality control check can take many formats but should result in a positive confirmation that the device being checked has undergone sanitisation. Examples of QC checks could be to power up the device / media to check a splash screen left in place by the overwriting software (if configured in that way). Another way could be to cross check the device / media's serial number with the central data base of overwriting certificates to ensure the serial number and an overwriting reference match. Finally, you could use specialist tools such as a HexViewer to check the device / media. This process should be documented, and a log kept.

For degaussing, in addition to the calibration checks in 3.4.9, operators should perform the same samples checks here by trying to read from drives which have undergone the degaussing technique.

For any other physical deformation technique, the outcome should be checked for consistency. For example, if drilling, checks must be made on the hole location to ensure the outcome meets the ADISA data capability requirements as per 3.4.1. e.g., for SSD that all NAND cells are deformed.

Guidance Notes (Continued)

3.4.13 This could be achieved by configuring the software overwriting tool to do 100% verification or to have a system fail safe where every asset should have the sanitisation confirmed before release to next stage of processing by integrating with the overwriting software management system.

Onsite services are where the data processing activities takes place on customer premises.

Essential

Ref	Criteria
3.5.1	All on-site services shall be governed by a customer engagement compliant with Section 2 Module 1.
3.5.2	Any sub-processors used shall be compliant with Section 2 Module 9.
3.5.3	There shall be a written method for services being undertaken which is to include a risk assessment.
3.5.4	Quality control procedures and testing samples shall be included within the written method for services being undertaken and comply with 3.5.23, 3.5.24 or 3.5.25 depending on the DIAL rating of the data controller.
3.5.5	All staff used to perform the service shall have undergone specific training in the use of any infrastructure and equipment used during the provision of the service.
3.5.6	All data sanitisation techniques undertaken on customer site shall be included in the Data Capability Statement and assessed as part of Section 3 Module 4.
3.5.7	Where software overwriting fails, hard drives or data carrying devices shall undergo a physical destruction process before being removed from customer site unless data controller authorises the release in writing.

Guidance Notes

3.5.3 The risk assessment should include both health and safety risks but also risk to the security of the operation such as uncontrolled working environments or power outages.

3.5.7 The physical destruction process may not be viewed as the final process applied to the device but could be viewed as a countermeasure to permit the media to be moved to the applicant's premises. This should be included within the method for services.

Identified Risks – Insider Theft, loss of control and health and safety at work		
Location where activities are to be carried out is uncontrolled and increases risk to the physical asset.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.5.8	**3.5.9**	**3.5.10**
Prior to work commencing, a recorded site survey shall be undertaken. This can be by the completion of a questionnaire and shall include security requirements for the processing area and also health and safety considerations for each location. It shall include the identification of the data processing location, access route to that location and power plan.	Prior to work commencing a formal site survey shall be undertaken by the applicant. This shall take place on site and shall include security requirements for the processing area and also health and safety considerations for each location. A risk assessment is to be included as part of this survey.	Work shall be carried out within a dedicated area within the customer or within a controlled environment set up by the applicant.

Guidance Notes

3.5.8 The site survey details can be captured in several ways including verbal (telephone) but should be recorded in a formal way such as on a system or specific form. Once captured this information should be incorporated into the written method for services being undertaken as per 3.5.3.

3.5.9 The written site survey should be carried out on site and be recorded in a formal way, such as on a system or specific form. Once captured this information should be incorporated into the written method for services being undertaken as per 3.5.3.

3.5.10 A dedicated area is defined as an area with clearly determined and defined boundaries which should include a secure perimeter. This would be assessed as per 3.5.9. Where no such location can be identified applicant should inform the customer in writing that they are unable to deliver the service to DIAL 3 but present the site survey from 3.5.9 including risk assessments with a recommended method statement for the work to be carried out. A DIAL 3 customer should sign off and approve this process before work can be carried out.

Identified Risk - Asset Loss		
Inventory control is poor leading to unclear transfer of custody from customer to applicant which leaves opportunity for unapproved data sanitisation and / or asset loss.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.5.11	**3.5.12**	**3.5.13**
There shall be a clearly defined transfer of custody of inventory from customer to applicant prior to work commencing. Inventory shall be tracked by a **box or consignment** count.	There shall be a clearly defined transfer of custody of inventory from customer to applicant prior to work commencing. Inventory shall be tracked by a count of **product types**.	An audit of media to be sanitised using a unique reference such as **serial number or asset tag** shall be carried out prior to work being commenced, approved by the customer, and verified at the end of the data processing activity.

Guidance Notes

3.5.11 An example of this would be an inventory counted by the number of sealed boxes which is detailed on paperwork and signed by the customer and the applicant. This follows the same principles as the transfer of custody outlined in 3.3.1.

3.5.12 An example of this would be an inventory counted by the number of products by type which is detailed on paperwork and signed by the customer and the applicant. This follows the same principles as the transfer of custody outlined in 3.3.2.

3.5.13 An example of this would be an inventory of media counted by unique identifiers such as serial numbers. This could be done by manually checking off against pre-printed lists OR by creating the list on site by scanning serial numbers. Provision should be made for dealing with devices which don't have serial numbers, or which would not scan. This follows the same principles as the transfer of custody outlined in 3.3.3.

This is where the data processing activity, media destruction, takes place within a vehicle which is taken to the customer's location to perform the service.

Identified Risk – Asset Loss		
Where the data processing is carried out within a vehicle the location of that vehicle might lead to a period of time where the physical assets are located outside of a physical perimeter increasing the risk to opportunist theft.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.5.14	**3.5.15**	**3.5.16**
Where work is carried out in a vehicle, a designated parking location for the vehicle shall be identified and recorded.	In addition to 3.5.14, there shall be a documented risk assessment determining the process for moving assets for destruction from customer site to vehicle.	In addition to 3.5.15, the vehicle shall be located with a secured location such as loading bay or private car park.

Guidance Notes

3.5.14 A designated parking location should include details of any parking restrictions, access limitations and details of whether the location is public or private.

3.5.15 The risk assessment should include detailed assessment of external risks posed by the location of the vehicle for the processing activity. If the vehicle is to be located in a public location, the risk assessment should include details of the procedural countermeasures put in place to manage the risk of asset exposure.

3.5.16 Where no secured location is available there should be evidence of the applicant informing the customer of this and providing them with the risk assessment from 3.5.15 for the customer to sign off.

Identified Risk – Asset Loss		
When undertaken inside a vehicle the processing activity is out of sight of the customer which increases the risk of insider theft or misappropriation of assets by the applicant.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.5.17	**3.5.18**	**3.5.19**
Shredding shall be carried out following a documented and controlled process.	In addition to 3.5.17, where work is carried out in a vehicle there shall be internal CCTV to film the asset input process. Each asset shall be scanned or photographed before being processed.	In addition to 3.5.18, the process shall be observed by a member of the customers' own staff.

Guidance Notes

3.5.17 A controlled process is defined as one where asset management is in place and physical security around the physical asset assessed.

3.5.18 The photographic evidence can be CCTV footage showing the asset input process as long as the assets are shown to the camera with the footage being good enough to identify the serial number of the drive.

3.5.19 Due to health and safety considerations the observation is not required to be carried out within the vehicle itself unless safe to do so. A written process document should be presented by the applicant to the customer detailed how observations will be allowed by the applicant when requested. These must comply with Health and Safety requirements for the operation of the shredder.

This is where data sanitisation using software overwriting is carried out by the applicant on the controller's premises. Typically, it is undertaken either direct to device, by utilisation of disk rigs brought on site or the creation of temporary networks within the customer location from which to run overwriting software.

Essential

Ref	Criteria
3.5.20	There shall be a written method statement which denotes how the applicant will manage the process on customer site. This is to include details of how data carrying, and data safe assets are to be segregated and how cross contamination is to be avoided.
3.5.21	Inventory to be processed shall be verified and signed into the control of applicant prior to overwriting by following 3.5.11, 3.5.12 or 3.5.13 depending on the DIAL level.
3.5.22	The software and means of deployment in a known configuration as per 3.4.5.

Guidance Notes

3.5.20 The method statement should include details of the technical set up of the data sanitisation solution but also the procedural set up of the service including inventory management and how the operational environment is to be controlled. It should also include how issues arising from operations are managed with a clear escalation process.

3.5.21 This inventory management is different to physical destruction as the assets are not physically destroyed and so the requirements for different DIAL numbers exceed the asset management for physical destruction as the devices are removed from site post sanitisation.

Section 3 Module 5 Onsite Services – Quality Control/Verification

There are different data sanitisation techniques which can be utilised. Some visually impact the media such as shredding whereas others may not. It is essential for the applicant to ensure the data sanitisation technique has been successful by performing a quality control / verification check. The quality control check for shredding is covered in 3.4.8 and all other data sanitisation techniques shall comply with the following.

Identified Risk – Data Breach		
Media or device did not undergo an approved means of sanitisation.		
Risk Treatment (Criterion)		
DIAL		
1	**2**	**3**
3.5.23	**3.5.24**	**3.5.25**
There shall be a documented quality control process, which will check a sample number of devices per month after the data sanitisation process has been complete. The minimum sample size shall be ten **per job** of all product types with a sampling log kept. Logs to be kept for a six-month period.	Same as 3.5.23.	In addition to 3.5.24 but **EVERY** device shall be checked to ensure the sanitisation technique was applied to it.

Guidance Notes

3.5.23 and 3.5.24 A quality control check can take many formats but should result in a positive confirmation that the device being checked has undergone sanitisation. Examples of QC checks could be to power up the device / media to check a splash screen left in place by the overwriting software (if configured in that way). Another way could be to cross check the device / media's serial number with the central data base of overwriting certificates to ensure the serial number and an overwriting reference match. Finally, you could use specialist tools such as a HexViewer to check the device / media. This process should be documented, and a log kept.

For degaussing, in addition to the calibration checks in 3.4.9, operators should perform the same samples checks here by trying to read from drives which have undergone the degaussing technique.

For any other physical deformation technique, the outcome should be checked for consistency. For example, if drilling, checks must be made on the hole location to ensure the outcome meets the ADISA data capability requirements as per 3.4.1. e.g., for SSD that all NAND cells are deformed.

Guidance Notes (Continued)

3.5.25 This could be achieved by configuring the software overwriting tool to do 100% verification or to have a system fail safe where every asset should have the sanitisation confirmed before release to next stage of processing by integrating with the overwriting software management system.

Essential

Ref	Criteria
3.5.26	In the absence of a written customer specification the applicant shall provide the customer with detailed audit reports to include, but not be limited to: • Serial Numbers of devices. • Make. • Model. • Evidence of end point sanitisation.
3.5.27	The applicant shall provide evidence of the verification and sign-off stages (to include a copy of a sample transfer of custody document).
3.5.28	The applicant shall provide the customer with copies of certificates of destruction and any waste compliance reports.

Guidance Notes

3.5.26 Evidence of end point sanitisation should include the inventory of the assets processed and the means of sanitisation.

3.5.27 The transfer of custody should show where the customer transfers custody to the applicant and how work is confirmed as being complete at the end of the service provision.

ICT Asset Recovery Standard 8.0

Section 4

Non-Data Services

Section Introduction

Within the ITAD sector there are additional services offered by the ITAD after the data processing activity, data sanitisation, has taken place. These are either recycling of products for material reclamation or the resale of products or components.

This section reviews these services at a high level to ensure the ITAD is operating good practice in both of these areas.

Section 4 Core Principles

- Compliance with Waste Management Legislation.
- Promotion of product reuse.

Essential

Ref	Criteria
4.1.1	Each applicant shall have all relevant environmental permits identified, verified and published by ADISA in their Waste Management Capabilities Statement.
4.1.2	Where the applicant passes waste to a third-party vendor for treatment, they shall be able to show documented evidence that their downstream partner holds all relevant permits and / or licenses to collect and treat waste within each region operated in. This record shall include validity dates of permits / licences held and copies of current permits / licences held shall be kept on file by the applicant.
4.1.3	Each collection which is designated as waste shall have the assets identified to the correct waste classification.
4.1.4	The applicant shall not export untreated waste from the country of origin.

Highly Desirable

Ref	Criteria
4.1.5	Where the applicant receives waste, they should keep records of all incoming movements of material by weight. Protocol weights are permitted.
4.1.6	The applicant should keep records of all outgoing waste movements by weight.
4.1.7	Where the applicant receives waste, each site should have personnel in place with suitable levels of qualification.

Guidance Notes

4.1.1 Waste Management Capabilities Statement template available from ADISA.

4.1.2 Documented evidence should be a controlled document listing all partners detailing what waste is sent to them, their permits / licences, and the validity of them.

4.1.3 The use of European Waste Category (EWC) codes is required for this.

4.1.4 The applicant can only issue waste to UK based companies correctly permitted by the Environment Agency.

Essential

Ref	Criteria
4.2.1	Each asset shall be tested to check that it is functional and fit for original purpose.
4.2.2	Each asset shall be graded against a written scale to confirm physical condition and records of grading kept with asset record.
4.2.3	Records of all assets either sold on or passed for further processing shall be kept. These records shall include unique tracking references of all equipment and the destination country. (Destination country shall not be a member of any embargoed list.)
4.2.4	All equipment sold to an end user shall include a warranty.
4.2.5	Any software installed shall hold a legal licence and be the current shipping version unless there is a technical reason for installing an older version.

Highly Desirable

Ref	Criteria
4.2.6	All equipment sold to an end user should include a minimum of a 28-days warranty.
4.2.7	During the auditing process a decision tree should be in place which allows an incomplete or non-functioning asset to undergo some remedial process and / or repair to make it ready for re-use.
4.2.8	Maximum opportunity for re-use of equipment should be in place by the holding of spares, accessories, and peripherals to make good damaged, non-functioning, or incomplete assets.
4.2.9	All equipment to be re-used should be cosmetically cleaned and where financially viable any missing components should be replaced to ensure maximum opportunity for re-use.

Guidance Notes

4.2.1 The testing process should be documented by product type so details of how each product is to be tested are communicated to operators.

4.2.2 Grading should be documented by product type or as a single grading for all products and this should be communicated to operators.

Phone: + 44 (1) 1582 361743

www.adisa.global
info@adisa.global